In the Claims:

Please replace claims 1, 5-7, 10-12, 18, 22-24, and 27-29, cancel claims 8, 9, 13, 15-17, 25, 26, 30, 32-34, and 40, and add new claims 42-43, all as shown below.

1. (Currently Amended): A security system for allowing a client to access a protected resource through an application container, the security system comprising:

an application container, which provides services for a protected resource, wherein the application container delegates authorization decisions to ~~the~~ a security service by passing an access request and a callback handler to the security service when the application container receives ~~an~~ the access request for a protected resource from a client;

context information, wherein the context information comprises one or more parameter values describing the access request, identity of the protected resource, and profile information describing the client ~~and can be retrieved from the application container by the security service using the callback handler~~;

~~said~~ the security service for making a decision to permit or deny the access request, wherein ~~the security service~~ a plurality of security plug-ins that implement an access decision interface are ~~includes providers that may be~~ plugged into the security service, and wherein the plurality of security plug-ins ~~providers~~ use the callback handler to request context information from the application container for the access request, and wherein the plurality of security plug-ins determine roles for which the client is entitled, and wherein association of the client to roles can be computed dynamically at runtime, and wherein depending on output from each security

plug-in ~~provider~~ the security service determines entitlements for the client to use with the protected resource; and

~~said~~ the security service is located at a first computer, and ~~said~~ the protected resource is located either at the ~~same~~ first computer or at a second computer~~; and~~

~~a resource interface for communicating permitted access requests to said protected resource~~.

2. (Previously Presented): The security system of claim 1 wherein the application container of claim 1 reads an application deployment description and registers the application deployment description within the security service.

3. (Canceled)

4. (Previously Presented): The security system of claim 2 wherein the application container is a Web Application container.

5. (Currently Amended): The security system of claim 1 wherein ~~the security service includes a plurality of access decision mechanisms for defining an access policy and~~ each of the plurality of security plug-ins ~~access decision mechanism~~ can determine ~~its own~~ a contributory decision to permit, deny, or abstain from the access request.

6. (Currently Amended): The security system of claim 5 wherein the security service further includes an access controller for transferring the access request to the plurality of security plug-ins ~~access decision mechanisms~~, and for combining the contributory decisions into an overall decision by the security service to permit or deny the access request.

7. (Currently Amended): The security system of claim 5 wherein one or more of the plurality of the security plug-ins ~~access decision mechanisms~~ represent a business function related authorization ~~access~~ policy.

8. – 9. (Canceled)

10. (Currently Amended): The security system of claim 5 wherein a deny or abstain by any one of the plurality of security plug-ins ~~access decision mechanisms~~ causes the security service to deny the access request.

11. (Currently Amended): The security system of claim 5 wherein an abstain by any one of the plurality of security plug-ins ~~access decision mechanisms~~ does not cause the security service to deny the access request.

12. (Currently Amended): The security system of claim 5 wherein the security service further includes security plug-ins that implement an audit interface ~~mechanism~~ for auditing the determinations of the plurality of access requests.

13. – 17. (Canceled)

18. (Currently Amended): A method of allowing a client to access a protected resource through an Application Container, the method comprising:

receiving at an application container, which provides services to the resources it contains, an access request from ~~said~~ the client to access ~~said~~ the protected resource;

communicating the access request from the application container to a security service with the access request and a callback handler, wherein the application container delegates authorization decisions to the security service by passing an access request and a callback handler to the security service when the application container receives an access request for the ~~a~~ protected resource from a client;

making a decision at the security service to permit or deny the access request, wherein ~~the security service includes~~ a plurality of security plug-ins that implement an access decision interface are ~~providers that may be~~ plugged into the security service;

using the callback handler at each security plug-in ~~provider~~ to request context information from the application container for the access request, wherein the context information comprises one or more parameter values describing the access request, identity of the protected resource, and profile information describing the client ~~and can be retrieved from the application container by the security service using the callback handler~~;

determining entitlements for the client to use with the protected resource depending on output from each security plug-in ~~provider~~, wherein the plurality of security plug-ins determine roles

for which the client is entitled, and wherein the association of the client to roles can be computed dynamically at runtime; and

communicating a permitted access request ~~through a resource interface~~ to the protected resource.

19. (Previously Presented): The method of claim 18 wherein the application container of claim 18 reads an application deployment description and registers the deployment description within the security service.

20. (Canceled)

21. (Previously Presented): The method of claim 19 wherein the application container is a Web Application container.

22. (Currently Amended): The method of claim 18 further comprising:

~~defining an access policy via a plurality of access decision mechanisms within the security service; and,~~

determining at each security plug-in ~~access decision mechanism~~ a contributory decision to permit, deny, or abstain from the access request.

23. (Currently Amended): The method of claim 22 further comprising:

transferring via an access controller the access request to the plurality of security plug-ins ~~access decision mechanisms~~, and combining the contributory decisions into an overall decision by the security service to permit or deny the access request.

24. (Currently Amended): The method of claim 22 wherein one or more of the plurality of the security plug-ins ~~access decision mechanisms~~ represent a business function related access policy.

25. -26. (Canceled)

27. (Currently Amended): The method of claim 22 wherein a deny or abstain by any one of the plurality of security plug-ins ~~access decision mechanisms~~ causes the security service to deny the access request.

28. (Currently Amended): The method of claim 22 wherein an abstain by any one of the plurality of security plug-ins ~~access decision mechanisms~~ does not cause the security service to deny the access request.

29. (Currently Amended): The method of claim 22 further comprising:

auditing ~~via an audit mechanism~~ the determinations of the plurality of access decision mechanisms.

30 – 34. (Canceled)

35. (Withdrawn): A method for determining user entitlements to access protected resources in a secure environment, comprising:

receiving an access request from a user application to access a protected resource, by invoking a security service with the access request and a callback;

determining user entitlements to access the protected resource, wherein the determining includes polling a plurality of security providers that may be plugged into the security service, and wherein the plurality of security providers use a callback handler to request context information from an application container for the access request;

making a decision at the security service based on the user entitlements to permit or deny the access request; and

the steps of either

(a) communicating a permitted access request to the protected resource, or

(b) denying a denied access request to the protected resource.

36. (Withdrawn): The method of claim 35 wherein if the access request is permitted, user entitlements also determine a type of access available to a user of the protected resource.

37. (Withdrawn): The method of claim 36 wherein the type of access includes any of view, modify, delete, or copy, any part or all of the protected resource.

38. (Withdrawn): The method of claim 35 wherein information about user entitlements can be communicated from a first security realm to a second security realm.

39. (Withdrawn): The method of claim 38 wherein additional information from a first security realm can be used to modify the user entitlements, prior to communicating the information about user entitlements from the first security realm to the second security realm.

40 – 41. (Canceled)

42. (New): The security system of claim 1, wherein computation of a dynamic role occurs immediately before an authorization decision for a protected resource.

43. (New): The security system of claim 18, wherein computation of a dynamic role occurs immediately before an authorization decision for a protected resource.